PTO/SB/21 (08-03)
Approved for use through 08/30/2003. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	10/708,988
Filing Date	04/06/2004
First Named Inventor	Wen-Long Chin
Art Unit	
Examiner Name	
Attorney Docket Number	ADMP0002USA

Total Number of Pages in This Submission: 3

ENCLOSURES *(Check all that apply)*

- [x] Fee Transmittal Form
- [ ] Fee Attached
- [ ] Amendment/Reply
- [ ] After Final
- [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
- [x] Certified Copy of Priority Document(s)
- [ ] Response to Missing Parts/ Incomplete Application
- [ ] Response to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
- [ ] After Allowance communication to Technology Center (TC)
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [ ] Other Enclosure(s) (please Identify below):

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Winston Hsu, Reg. No.: 41,526
Signature	Winston Hsu
Date	4/12/2004

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Typed or printed name			
Signature		Date	

PTO/SB/17 (10-03)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

FEE TRANSMITTAL for FY 2004

Effective 10/01/2003. Patent fees are subject to annual revision.

☑ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 0.00

Complete if Known	
Application Number	10/708,988
Filing Date	04/06/2004
First Named Inventor	Wen-Long Chin
Examiner Name	
Art Unit	
Attorney Docket No.	ADMP0002USA

METHOD OF PAYMENT *(check all that apply)*

☐ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☑ Deposit Account:

Deposit Account Number: 50-0801

Deposit Account Name: North America International Patent Office

The Director is authorized to: *(check all that apply)*

☑ Charge fee(s) indicated below ☑ Credit any overpayments

☑ Charge any additional fee(s) or any underpayment of fee(s)

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	770	2001	385	Utility filing fee	
1002	340	2002	170	Design filing fee	
1003	530	2003	265	Plant filing fee	
1004	770	2004	385	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	

SUBTOTAL (1) ($) 0.00

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

		Extra Claims		Fee from below	Fee Paid
Total Claims		-20** =		X	=
Independent Claims		- 3** =		X	=
Multiple Dependent					=

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	86	2201	43	Independent claims in excess of 3
1203	290	2203	145	Multiple dependent claim, if not paid
1204	86	2204	43	** Reissue independent claims over original patent
1205	18	2205	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 0.00

***or number previously paid, if greater; For Reissues, see above*

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	0.00
1252	420	2252	210	Extension for reply within second month	
1253	950	2253	475	Extension for reply within third month	
1254	1,480	2254	740	Extension for reply within fourth month	
1255	2,010	2255	1,005	Extension for reply within fifth month	
1401	330	2401	165	Notice of Appeal	
1402	330	2402	165	Filing a brief in support of an appeal	
1403	290	2403	145	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive - unavoidable	
1453	1,330	2453	665	Petition to revive - unintentional	
1501	1,330	2501	665	Utility issue fee (or reissue)	
1502	480	2502	240	Design issue fee	
1503	640	2503	320	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	770	2809	385	Filing a submission after final rejection (37 CFR 1.129(a))	
1810	770	2810	385	For each additional invention to be examined (37 CFR 1.129(b))	
1801	770	2801	385	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($) 0.00

SUBMITTED BY				(Complete *(if applicable)*)	
Name (Print/Type)	Winston Hsu	*Registration No. (Attorney/Agent)*	41,526	*Telephone*	886289237350
Signature	Winston Hsu			*Date*	4/12/2004

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

This collection of information is required by 37 CFR 1.17 and 1.27. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/02B (11-00)
Approved for use through 10/31/2002. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

DECLARATION — Supplemental Priority Data Sheet

Additional foreign applications:

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached? YES	NO
093100386	Taiwan R.O.C	01/07/2004	☐	☑	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐

中華民國經濟部智慧財產局

INTELLECTUAL PROPERTY OFFICE
MINISTRY OF ECONOMIC AFFAIRS
REPUBLIC OF CHINA

茲證明所附文件，係本局存檔中原申請案的副本，正確無訛，
其申請資料如下 ：

This is to certify that annexed is a true copy from the records of this office of the application as originally filed which is identified hereunder :

申　請　日 ： 西元 2004 年 01 月 07 日
Application Date

申　請　案　號 ： 093100386
Application No.

申　請　人 ： 上元科技股份有限公司
Applicant(s)

局　　長
Director General

蔡練生

發文日期： 西元2004 年 3 月 31 日
Issue Date

發文字號： 09320296310
Serial No.

申請日期：	IPC分類
申請案號：	

(以上各欄由本局填註)

發明專利說明書

一、發明名稱	中文	使用超長指令字元架構之處理器執行進階密碼標準之方法
	英文	METHOD FOR IMPLEMENTING ADVANCED ENCRYPTION STANDARDS BY A VERY LONG INSTRUCTION WORD ARCHITECTURE PROCESSOR
二、發明人(共2人)	姓名(中文)	1.卿文龍
	姓名(英文)	1.CHIN, WEN-LONG
	國籍(中英文)	1.中華民國 TW
	住居所(中文)	1.新竹縣竹北市中華路七九九之八號三樓
	住居所(英文)	1.3F, No. 799-8, Chung-Hwa Rd., Chu-Pei City, Hsin-Chu Hsien, Taiwan, R.O.C.
三、申請人(共1人)	名稱或姓名(中文)	1.上元科技股份有限公司
	名稱或姓名(英文)	1.ADMTEK INCORPORATED
	國籍(中英文)	1.中華民國 TW
	住居所(營業所)(中文)	1.新竹市科學工業園區力行路2號2樓 (本地址與前向貴局申請者相同)
	住居所(營業所)(英文)	1.2F, No. 2, Li-Hsin Rd., Science-based Industrial Park, Hsin-Chu City, Taiwan, R.O.C.
	代表人(中文)	1.盧崑瑞
	代表人(英文)	1.LU, KUEN-RUEY

申請日期：	IPC分類
申請案號：	

(以上各欄由本局填註)

發明專利說明書

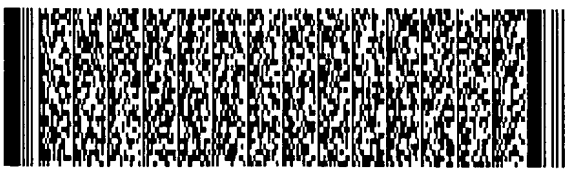
一、發明名稱	中 文	
	英 文	
二、發明人(共2人)	姓 名(中文)	2.劉廣治
	姓 名(英文)	2.LIU, KUANG-CHIH
	國 籍(中英文)	2.中華民國 TW
	住居所(中 文)	2.新竹市香山區墩豐路三十巷十二號
	住居所(英 文)	2.No. 12, Lane 30, Tun-Feng Rd., Hsiang-Shan District, Hsin-Chu City, Taiwan, R.O.C.
三、申請人(共1人)	名稱或姓 名(中文)	
	名稱或姓 名(英文)	
	國 籍(中英文)	
	住居所(營業所)(中 文)	
	住居所(營業所)(英 文)	
	代表人(中文)	
	代表人(英文)	

四、中文發明摘要　(發明名稱：使用超長指令字元架構之處理器執行進階密碼標準之方法)

本發明提供一使用超長指令字元架構之處理器執行進階密碼標準之方法。該方法包含由該處理器之指令輸入埠輸入執行進階密碼標準之指令後傳至該處理器之指令解碼與排程器進行解碼及排程；根據該解碼及排程後之指令控制該處理器之複數個多工器之輸出，由該處理器之第一暫存器及算術邏輯單元輸入該多工器之複數筆資料中之複數筆至該算術邏輯單元及該第一暫存器，以及控制該算術邏輯單元執行運算功能；最後將該算術邏輯單元執行運算功能產生之資料輸入該複數個多工器。本發明之方法使得進階密碼標準之複數個相異模式之加解密功能可在同一使用超長指令字元架構之處理器上處理及執行。

五、英文發明摘要　(發明名稱：METHOD FOR IMPLEMENTING ADVANCED ENCRYPTION STANDARDS BY A VERY LONG INSTRUCTION WORD ARCHITECTURE PROCESSOR)

Abstract:
A method for implementing Advanced Encryption Standards (AES) by a very long instruction word (VLIW) architecture processor. The method includes inputting the instructions for AES into the processor, decoding and scheduling the input instructions, controlling at least one of a plurality of multiplexers to output data from a



四、中文發明摘要　（發明名稱：使用超長指令字元架構之處理器執行進階密碼標準之方法）

五、英文發明摘要　（發明名稱：METHOD FOR IMPLEMENTING ADVANCED ENCRYPTION STANDARDS BY A VERY LONG INSTRUCTION WORD ARCHITECTURE PROCESSOR）

first register of the processor and/or a arithmetic logic unit to the first register and/or the arithmetic logic unit according to the decoded and scheduled instructions, controlling the arithmetic logic unit to perform operations, and output results of the operations to the plurality of the multiplexers.

六、指定代表圖

(一)、本案代表圖為：第 __一 ___圖

(二)、本案代表圖之元件代表符號簡單說明：

100　超長指令字元架構之處理器

110　緩衝區

120　第一暫存區

130　輸出輸入控制器

140　算術邏輯單元

141, 142, 143　輸入埠

146, 147　輸出埠

148　基礎邏輯運算單元

149　特殊進階密碼標準指令單元

152, 154, 156　多工器

160　指令輸入埠

170　指令暫存器

180　指令解碼與排程器

一、本案已向

國家(地區)申請專利	申請日期	案號	主張專利法第二十四條第一項優先權

無

二、□主張專利法第二十五條之一第一項優先權:

申請案號:

無

日期:

三、主張本案係符合專利法第二十條第一項□第一款但書或□第二款但書規定之期間

日期:

四、□有關微生物已寄存於國外:

寄存國家:

寄存機構: 無

寄存日期:

寄存號碼:

□有關微生物已寄存於國內(本局所指定之寄存機構):

寄存機構:

寄存日期: 無

寄存號碼:

□熟習該項技術者易於獲得,不須寄存。

五、發明說明 (1)

【發明所屬之技術領域】

本發明提供一執行進階密碼標準之方法，尤指一使用超長指令字元架構之處理器來執行進階密碼標準之方法。

【先前技術】

進階密碼標準（Advanced Encryption Standards, AES）是美國聯邦資訊處理標準（Federal Information Processing Standards, FIPS）所認可的密碼演算法標準，其可用來保護電子資料。進階密碼標準演算法是一對稱之加解密標準，其可對資訊進行加密而成為密文（ciphertext），再將密文解密而還原成原本的明文（plaintext）以保障該文件之安全。AES演算法可使用128位元長度、192位元長度、以及256位元長度的密鑰（cryptographic key）對128位元長度的資料塊（data block）進行加解密。相較於另一習知之資料密碼標準（Data Encryption Standards, DES），進階密碼標準能提供更高的安全性。

進階密碼標準起初是提供美國聯邦政府部門局處官員於需要加密保護敏感的資訊時使用，而現在進階密碼標準則也可供美國聯邦政府以外的商業或個人組織使用。針對不同的應用需要，進階密碼標準具有不同的操作模

式，現在常用的有二，分別是偏碼表（Offset Code Book，OCB）模式以及Counter mode with CBC MAC (CCM)模式。目前已有許多以硬接線（hard-wired）實現進階密碼標準的方式，而因為進階密碼標準演算法中有許多查詢表（look up table）及複雜的運算電路，所以這些實現進階密碼標準演算法的晶片電路的面積都非常大。為了能加快運算速度，許多用來執行進階密碼標準演算法的電路在設計時會將各迴圈展開以加快系統效能，如此一來這些晶片電路的尺寸又會再加大，即成本會上升。由此我們可知，於實施進階密碼標準時，所付出的成本與能得到的效能間無法兩全而必須互相妥協以找到一平衡點。就算不惜成本而將每一迴圈都展開以製成一最快的進階密碼標準電路，當進階密碼標準演算法應用到不同的實際情況中時，會需要不同的操作模式，而這些操作模式彼此間互相差異之大以致於在原本為單一模式設計的電路上操作時，效能會有很大的衰減，甚至必須重新設計不同的電路來執行這些不同模式的進階密碼標準演算法。以硬體電路設計實現AES加解密功能者之不具應用上的彈性由此可見一斑。

除了以硬體實現進階密碼標準演算法，習知技術中亦有以軟體執行進階密碼標準之加解密功能者。此類進階密碼標準技術是在一般通用性（general purpose)的處理器上以程式碼執行進階密碼標準的加解密功能。像這樣以

軟體執行進階密碼標準的加解密功能的好處在於其可在相同的處理器上，以不同的程式執行不同模式的進階密碼標準之加解密功能；不需要改變或提供更多的硬體資源，而仍可實現不同模式的AES加解密功能，因而可節省成本。然而，以軟體執行進階密碼標準之加解密功能的速度較慢，當使用者或是系統的需求較高時，即可明顯看出以軟體執行進階密碼標準之加解密功能者於速度上的弱勢。

【發明內容】

因此本發明提出一種使用超長指令字元（Very Long Instruction Word, VLIW）架構之處理器以執行進階密碼標準（Advanced Encryption Standards, AES）之方法，該方法在一固定之使用超長指令字元架構之處理器之上，配合以不同的指令即可執行不同模式的AES加解密功能，以克服上述習知技術中的問題。

根據本發明之申請專利範圍，係揭露一種一種使用超長指令字元（Very Long Instruction Word, VLIW）架構的處理器執行進階密碼標準（Advanced Encryption Standards, AES）之方法，該處理器包含：一緩衝區，用來存放資料；一第一暫存器，電連接至該緩衝區，該第一暫存器包含複數個輸出埠及複數個輸入埠；一輸出

輸入控制器，電連接至該緩衝區及該第一暫存器，用來控制資料由該第一暫存器傳送至該緩衝區或由該緩衝區傳送至該第一暫存器；一算術邏輯單元（arithmetic logic unit, ALU），其包含：複數個輸入埠，複數個輸出埠，一基礎邏輯運算單元，以及一特殊進階密碼標準指令單元。該處理器另包含複數個多工器，其中每一個多工器皆包含複數個輸入埠及一個輸出埠，其中該多工器之輸入埠電連接至該第一暫存器之輸出埠或該算術邏輯單元之輸出埠，以及該多工器之輸出埠電連接至該算術邏輯單元之輸入埠及該第一暫存器之輸入埠；一指令輸入埠，用來接收執行進階密碼標準之指令；一指令暫存器，電連接至該指令輸入埠，用來暫存由該指令輸入埠所輸入之指令；以及一指令解碼與排程器，電連接至該指令暫存器、該複數個多工器以及該算術邏輯單元，用來將由該指令暫存器所傳來之指令解碼及排程，控制該複數個多工器之輸出至該算術邏輯單元，以及控制該算術邏輯單元執行運算功能。本發明之方法係由該指令輸入埠輸入執行進階密碼標準之指令後傳至該指令暫存器，再傳至該指令解碼與排程器進行解碼及排程；根據該解碼及排程後之指令控制該複數個多工器中至少一多工器輸出由該第一暫存器及該算術邏輯單元輸入該多工器之複數筆資料中之一筆至該算術邏輯單元及該第一暫存器，以及控制該算術邏輯單元執行運算功能；最後將該算術邏輯單元執行運算功能產生之資料輸入該複數個

多工器。

【實施方式】

請參閱圖一。圖一為本發明之方法所使用超長指令字元(Very Long Instruction Word, VLIW)架構的處理器示意圖。100為一超長指令字元架構之處理器，其包含：一緩衝區110，用來存放資料；一第一暫存器120，電連接至緩衝區110，可將資料輸出之緩衝區110或接收由緩衝區110所傳來之資料；一輸出輸入控制器130，電連接至緩衝區110及第一暫存器120，用來控制資料由第一暫存器120送至緩衝區110或由緩衝區110傳送至第一暫存器120；一算術邏輯單元(arithmetic logic unit, ALU)140，其包含：複數個輸入埠141、142及143，複數個輸出埠146及147，一基礎邏輯運算單元148用以執行基礎邏輯運算功能，以及一特殊進階密碼標準指令單元149用以執行根據進階密碼標準所設計之特殊邏輯運算功能；其中第一暫存器120包含有複數個輸出埠及複數個輸入埠。處理器100還包含複數個多工器152、154及156，其中每一個多工器皆包含複數個輸入埠及一個輸出埠，其中該多工器之可由第一暫存器120或算術邏輯單元140接收資料，並且該多工器可將資料輸出至算術邏輯單元140及第一暫存器120；一指令輸入埠160，用來接收執行進階密碼標準之指令；一指令暫存器170，電連接至指令輸入埠

160，用來暫存由指令輸入埠160所輸入之指令；以及一指令解碼與排程器180，電連接至指令暫存器170、該複數個多工器152、154及156、以及算術邏輯單元140，指令解碼與排程器180係用來將由指令暫存器170所傳來之指令解碼及排程，控制該複數個多工器中至少一多工器輸出輸入該多工器之複數筆資料中之一筆至算術邏輯單元140以及控制算術邏輯單元140執行運算功能。當使用本發明之執行進階密碼標準之方法時，首先以輸出輸入控制埠130控制緩衝區110與第一暫存區120間資料之傳輸方向，將欲待以進階密碼標準進行加密之一筆明文資料以及加密用之密鑰由緩衝區110輸出至第一暫存區120暫存。本發明之方法係將執行進階密碼標準之指令輸入至指令輸入埠160後將該指令傳至指令暫存器170中暫存，再將指令暫存器170中之指令傳至指令解碼與排程器180；指令解碼與排程器170會將由指令暫存器170所傳來之指令解碼及排程後輸出至複數個多工器152、154及156與算術邏輯單元140，以控制該複數個多工器中至少一多工器輸出由第一暫存器120及算術邏輯單元140輸入該多工器之複數筆資料中之一筆至算術邏輯單元140及第一暫存器120，以及控制算術邏輯單元140執行相對於該解碼及排程後之指令之運算功能。算術邏輯單元140執行運算功能而產生之資料會輸入該複數個多工器；而當所有指令執行完畢，即將一筆明文以進階密碼標準完成加密或將一筆密文以進階密碼標準完成解密後，該筆完成加密

或解密之資料將由多工器輸出至第一暫存器120，輸出輸入控制埠再控制該筆資料由第一暫存器120輸出至緩衝區110。

請參閱圖二。圖二為本發明之方法使用超長指令字元架構之處理器執行進階密碼標準之流程圖。本發明之方法包括以下步驟：

步驟200：開始執行進階密碼標準之加解密功能；
步驟210：輸出輸入控制埠130控制緩衝區110與第一暫存器120間之資料傳輸方向為由緩衝區110傳至第一暫存器120；
步驟220：將待加密/解密之明文/密文資料以及加密/解密用之密鑰由緩衝區110輸出至第一暫存區120；
步驟230：將第一暫存區120中暫存之資料傳至該複數個多工器；
步驟240：將執行進階密碼標準加密/解密功能之指令輸入指令輸入埠160；
步驟250：將輸入指令輸入埠160之指令傳至指令暫存器170；
步驟260：將輸入指令暫存器170之指令傳至指令解碼與排程器180；
步驟270：將輸入指令解碼與排程器180之指令解碼及排程；

步驟 280：根據指令解碼與排程器 180解碼及排程後之指令，控制該複數個多工器中至少一多工器輸出由第一暫存器 120及算術邏輯單元 140輸入該多工器之複數筆資料中之一筆資料至算術邏輯單元 140及第一暫存器 120；

步驟 290：若加密 /解密功能已完成，則執行步驟 300；若加密 /解密功能尚未完成，則根據指令解碼與排程器 180解碼及排程後之指令控制算術邏輯單元 140執行運算功能；

步驟 300：將算術邏輯單元 140根據指令解碼與排程器 180解碼及排程後之指令所執行之運算結果輸出至複數個多工器 152、154及 156；執行步驟 270；

步驟 310：輸出輸入控制埠 130控制緩衝區 110與第一暫存器 120間之資料傳輸方向為由第一暫存器 120傳至緩衝區 110；

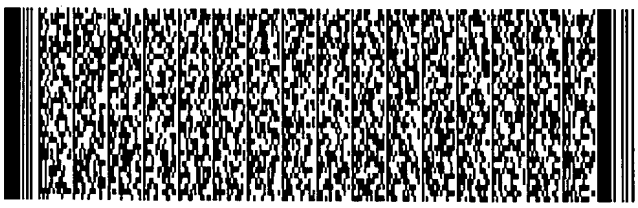
步驟 320：將已完成加密 /解密之資料由第一暫存器 120傳至緩衝區 110；

步驟 330：完成進階密碼標準之加解密。

以上為本發明之使用超長指令字元（Very Long Instruction Word, VLIW）架構之處理器執行進階密碼標準（Advanced Encryption Standards, AES）之方法之實施流程，其中當搭配相對之指令時，該方法可執行 128位元長度、192位元長度、以及 256位元長度之進階密碼標準（AES-128, AES-192, AES-256）之加密及解密功

能。本發明之方法利用一使用超長指令字元架構之處理器執行進階密碼標準，其中該處理器可設計成讓本發明之方法能平行處理複數筆資料或平行處理複數個指令，例如可同時產生進階密碼標準之密鑰以及使用進階密碼標準對一筆明文資料進行加密，同時產生進階密碼標準之密鑰以及使用進階密碼標準對複數筆明文資料進行加密；以及使用同樣的密鑰同時對複數筆資料進行加密。配合本發明之方法所使用之處理器之平行處理之能力，本發明之方法可於執行一替換位元組換列-1（substitute byte shift row 1, SBSR1）指令時同時處理暫存於第一暫存器120所包含之暫存器R0、暫存器R1、暫存器R2及暫存器R3之最低有效位元組（least significant byte, LSB）及第二低有效位元組共八個位元組之資料；於執行一替換位元組換列-2（substitute byte shift row 2, SBSR2）指令時同時處理暫存於該暫存器R0、該暫存器R1、該暫存器R2及該暫存器R3之最高有效位元組（most significant byte, MSB）及第二高有效位元組共八個位元組之資料；於執行一混行增加循環密鑰-1（mix column add round key 1, MIXADK1）指令時同時處理暫存於該暫存器R0及該暫存器R1之資料；於執行一混行增加循環密鑰-2（mix column add round key 2, MIXADK2）指令時同時處理暫存於該暫存器R2及該暫存器R3之資料；於執行一逆替換位元組換列-1（inverse substitute byte shift row 1, INVSBSR1）


指令時同時處理暫存於該暫存器R0、該暫存器R1、該暫存器R2及該暫存器R3之最低有效位元組（least significant byte, LSB）及第二低有效位元組共八個位元組之資料；於執行一逆替換位元組換列-2（inverse substitute byte shift row 2, INVSBSR2）指令時同時處理暫存於該暫存器R0、該暫存器R1、該暫存器R2及該暫存器R3之最高有效位元組（most significant byte, MSB）及第二高有效位元組共八個位元組之資料；於執行一逆混行增加循環密鑰-1（inverse mix column add round key 1, MIXADK1）指令時同時處理暫存於該暫存器R0及該暫存器R1之資料；於執行一逆混行增加循環密鑰-2（inverse mix column add round key 2, MIXADK2）指令時同時處理暫存於該暫存器R2及該暫存器R3之資料；於執行一替換位元組換列-3（substitute byte shift row 3, SBSR3）指令時同時處理暫存於第一暫存器120所包含之暫存器R20、暫存器R21、暫存器R22及暫存器R23之最低有效位元組（least significant byte, LSB）及第二低有效位元組共八個位元組之資料；於執行一替換位元組換列-4（substitute byte shift row 4, SBSR4）指令時同時處理暫存於該暫存器R20、該暫存器R21、該暫存器R22及該暫存器R23之最高有效位元組（most significant byte, MSB）及第二高有效位元組共八個位元組之資料；於執行一混行增加循環密鑰-3（mix column add round key 3, MIXADK3）指令時同時



處理暫存於該暫存器R20及該暫存器R21之資料；於執行一混行增加循環密鑰-4(mix column add round key 4, MIXADK4) 指令時同時處理暫存於該暫存器R22及該暫存器R23之資料；於執行一逆替換位元組換列-3(inverse substitute byte shift row 3, INVSBSR3) 指令時同時處理暫存於該暫存器R20、該暫存器R21、該暫存器R22及該暫存器R23之最低有效位元組(least significant byte, LSB) 及第二低有效位元組共八個位元組之資料；以及於執行一逆替換位元組換列-4(inverse substitute byte shift row 4, INVSBSR4) 指令時同時處理暫存於該暫存器R20、該暫存器R21、該暫存器R22及該暫存器R3之最高有效位元組(most significant byte, MSB) 及第二高有效位元組共八個位元組之資料。除了以平行處理提高實施加解密之效率外，只要將進階密碼標準之不同模式所對應之指令輸入本發明之方法所使用之使用超長指令字元架構之處理器，本發明之方法即可完成不同模式如偏碼表(Offset Code Book , OCB) 模式以及CCM模式之進階密碼標準之加解密功能，有效克服習知技術中需以不同硬體以實施不同模式之進階密碼標準之加解密之不便。

綜上所述，本發明提出之使用超長指令字元架構之處理器執行進階密碼標準之方法可搭配不同模式之指令以實現不同模式之加解密功能，充份改善習知技術中以硬體

實現進階密碼標準時無法同時適用於不同模式之加解密功能之缺點；而平行處理之硬體設計又使得本發明之方法較以純軟體實現進階密碼標準之習知技術來得速度快又有效率。

以上所述僅為本發明之較佳實施例，凡依本發明申請專利範圍所做之均等變化與修飾，皆應屬本發明專利之涵蓋範圍。

圖式之簡單說明

圖一為本發明之方法所利用之使用超長指令字元架構的處理器示意圖。

圖二為本發明之方法執行進階密碼標準之流程圖。

圖式之符號說明

100　超長指令字元架構之處理器
110　緩衝區
120　第一暫存區
130　輸出輸入控制器
140　算術邏輯單元
141, 142, 143　輸入埠
146, 147　輸出埠
148　基礎邏輯運算單元
149　特殊進階密碼標準指令單元
152, 154, 156　多工器
160　指令輸入埠
170　指令暫存器
180　指令解碼與排程器

六、申請專利範圍

1. 一種使用超長指令字元（Very Long Instruction Word, VLIW）架構之處理器執行進階密碼標準（Advanced Encryption Standards, AES）之方法，該處理器包含：

一緩衝區，用來存放資料；

一第一暫存器，電連接至該緩衝區，該第一暫存器包含複數個輸出埠及複數個輸入埠；

一輸出輸入控制器，電連接至該緩衝區及該第一暫存器，用來控制資料由該第一暫存器傳送至該緩衝區或由該緩衝區傳送至該第一暫存器；

一算術邏輯單元（arithmetic logic unit, ALU），其包含：

複數個輸入埠：

複數個輸出埠；

一基礎邏輯運算單元，用來執行基礎邏輯運算功能；以及

一特殊進階密碼標準指令單元，用來執行根據進階密碼標準所設計之特殊邏輯運算功能；

複數個多工器，其中每一個多工器皆包含複數個輸入埠及一個輸出埠，其中該多工器之輸入埠電連接至該第一暫存器之輸出埠或該算術邏輯單元之輸出埠，以及該多工器之輸出埠電連接至該算術邏輯單元之輸入埠及該第一暫存器之輸入埠；

一指令輸入埠，用來接收執行進階密碼標準之指令；

六、申請專利範圍

一指令暫存器，電連接至該指令輸入埠，用來暫存由該指令輸入埠所輸入之指令；以及

一指令解碼與排程器，電連接至該指令暫存器、該複數個多工器以及該算術邏輯單元，用來將由該指令暫存器所傳來之指令解碼及排程，控制該複數個多工器中至少一多工器輸出輸入該多工器之複數筆資料中之一筆至該算術邏輯單元以及控制該算術邏輯單元執行運算功能；

該方法包含：

(a) 由該指令輸入埠輸入執行進階密碼標準之指令；

(b) 將輸入該指令輸入埠之指令傳至該指令暫存器；

(c) 將輸入該該指令暫存器之指令傳至該指令解碼與排程器；

(d) 將該指令暫存器傳至該指令解碼與排程器之指令解碼及排程；

(e) 根據該指令解碼與排程器解碼及排程後之指令，控制該複數個多工器中至少一多工器輸出由該第一暫存器及該算術邏輯單元輸入該多工器之複數筆資料中之一筆至該算術邏輯單元及該第一暫存器，以及控制該算術邏輯單元執行運算功能；以及

(f) 將該算術邏輯單元執行運算功能產生之資料輸入該複數個多工器。

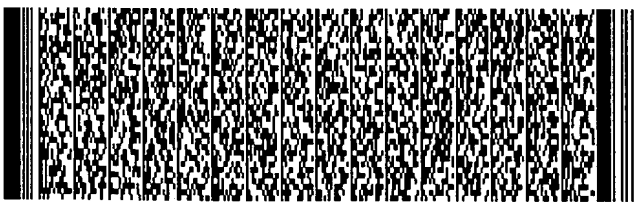
2. 如申請專利範圍第1項之方法，其可處理及執行進階密碼標準之複數個相異模式之指令。

3. 如申請專利範圍第1項之方法，其可執行128位元長度、192位元長度、以及256位元長度之進階密碼標準（AES-128, AES-192, AES-256）之加密及解密功能。

4. 如申請專利範圍第1項之方法，其中該處理器之第一暫存器包含複數個暫存器，該複數個暫存器包含一暫存器R0，一暫存器R1，一暫存器R2以及一暫存器R3，該方法可執行一替換位元組換列-1（substitute byte shift row 1, SBSR1）指令，且該方法於執行該替換位元組換列-1指令時係同時處理暫存於該暫存器R0、該暫存器R1、該暫存器R2及該暫存器R3之最低有效位元組（least significant byte, LSB）及第二低有效位元組共八個位元組之資料。

5. 如申請專利範圍第4項之方法，其可執行一替換位元組換列-2（substitute byte shift row 2, SBSR2）指令，且該方法於該執行替換位元組換列-2指令時係同時處理暫存於該暫存器R0、該暫存器R1、該暫存器R2及該暫存器R3之最高有效位元組（most significant byte, MSB）及第二高有效位元組共八個位元組之資料。

6. 如申請專利範圍第1項之方法，其中該處理器之第一暫存器包含複數個暫存器，該複數個暫存器包含一暫存



器R0，一暫存器R1，一暫存器R2以及一暫存器R3，該方法可執行一混行增加循環密鑰-1(mix column add round key 1, MIXADK1)指令，且該方法於執行該混行增加循環密鑰-1指令時係同時處理暫存於該暫存器R0及該暫存器R1之資料。

7. 如申請專利範圍第6項之方法，其可執行一混行增加循環密鑰-2(mix column add round key 2, MIXADK2)指令，且該方法於執行該混行增加循環密鑰-2指令時係同時處理暫存於該暫存器R2及該暫存器R3之資料。

8. 如申請專利範圍第1項之方法，其可同時產生進階密碼標準之密鑰以及使用進階密碼標準對一筆明文(plaintext)資料進行加密。

9. 如申請專利範圍第1項之方法，其可同時產生進階密碼標準之密鑰以及使用進階密碼標準對複數筆明文資料進行加密。

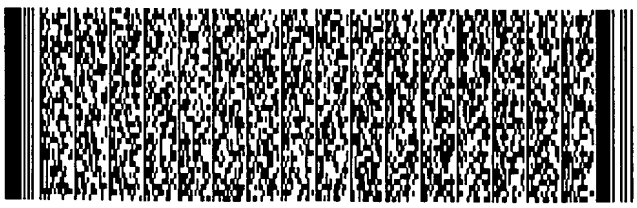
10. 如申請專利範圍第1項之方法，其中該處理器之第一暫存器包含複數個暫存器，該複數個暫存器包含一暫存器R0，一暫存器R1，一暫存器R2以及一暫存器R3，該方法可執行一逆替換位元組換列-1(inverse substitute byte shift row 1, INVSBSR1)指令，且該方法於執行

該逆替換位元組換列-1指令時係同時處理暫存於該暫存器R0、該暫存器R1、該暫存器R2及該暫存器R3之最低有效位元組（least significant byte, LSB）及第二低有效位元組共八個位元組之資料。

11. 如申請專利範圍第10項之方法，其可執行一逆替換位元組換列-2（inverse substitute byte shift row 2, INVSBSR2）指令，且該方法於執行該逆替換位元組換列-2指令時係同時處理暫存於該暫存器R0、該暫存器R1、該暫存器R2及該暫存器R3之最高有效位元組（most significant byte, MSB）及第二高有效位元組共八個位元組之資料。

12. 如申請專利範圍第1項之方法，其中該處理器之第一暫存器包含複數個暫存器，該複數個暫存器包含一暫存器R0，一暫存器R1，一暫存器R2以及一暫存器R3，該方法可執行一逆混行增加循環密鑰-1（inverse mix column add round key 1, MIXADK1）指令，且該方法於執行該逆混行增加循環密鑰-1指令時係同時處理暫存於該暫存器R0及該暫存器R1之資料。

13. 如申請專利範圍第12項之方法，其可執行一逆混行增加循環密鑰-2（inverse mix column add round key 2, MIXADK2）指令，且該方法於執行該逆混行增加循環

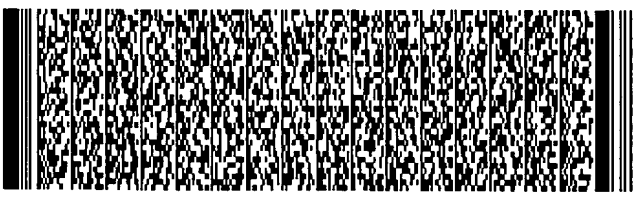


密鑰-2指令時係同時處理暫存於該暫存器R2及該暫存器R3之資料。

14. 如申請專利範圍第1項之方法，其中該處理器之第一暫存器包含複數個暫存器，該複數個暫存器包含一暫存器R20，一暫存器R21，一暫存器R22以及一暫存器R23，該方法可執行一替換位元組換列-3(substitute byte shift row 3, SBSR3)指令，且該方法於執行該替換位元組換列-3指令時係同時處理暫存於該暫存器R20、該暫存器R21、該暫存器R22及該暫存器R23之最低有效位元組(least significant byte, LSB)及第二低有效位元組共八個位元組之資料。

15. 如申請專利範圍第14項之方法，其可執行一替換位元組換列-4(substitute byte shift row 4, SBSR4)指令，且該方法於執行該替換位元組換列-4指令時係同時處理暫存於該暫存器R20、該暫存器R21、該暫存器R22及該暫存器R23之最高有效位元組(most significant byte, MSB)及第二高有效位元組共八個位元組之資料。

16. 如申請專利範圍第1項之方法，其中該處理器之第一暫存器包含複數個暫存器，該複數個暫存器包含一暫存器R20，一暫存器R21，一暫存器R22以及一暫存器R23，該方法可執行一混行增加循環密鑰-3(mix column add

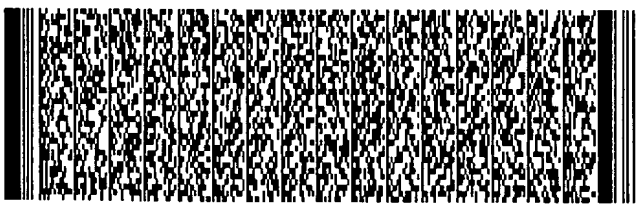


round key 3, MIXADK3) 指令，且該方法於執行該混行增加循環密鑰-3指令時係同時處理暫存於該暫存器R20及該暫存器R21之資料。

17. 如申請專利範圍第16項之方法，其可執行一混行增加循環密鑰-4(mix column add round key 4, MIXADK4) 指令，且該方法於執行該混行增加循環密鑰-4指令時係同時處理暫存於該暫存器R22及該暫存器R23之資料。

18. 如申請專利範圍第1項之方法，其中該處理器之第一暫存器包含複數個暫存器，該複數個暫存器包含一暫存器R20，一暫存器R21，一暫存器R22以及一暫存器R23，該方法可執行一逆替換位元組換列-3(inverse substitute byte shift row 3, INVSBSR3) 指令，且該方法於執行該逆替換位元組換列-3指令時係同時處理暫存於該暫存器R20、該暫存器R21、該暫存器R22及該暫存器R23之最低有效位元組(least significant byte, LSB) 及第二低有效位元組共八個位元組之資料。

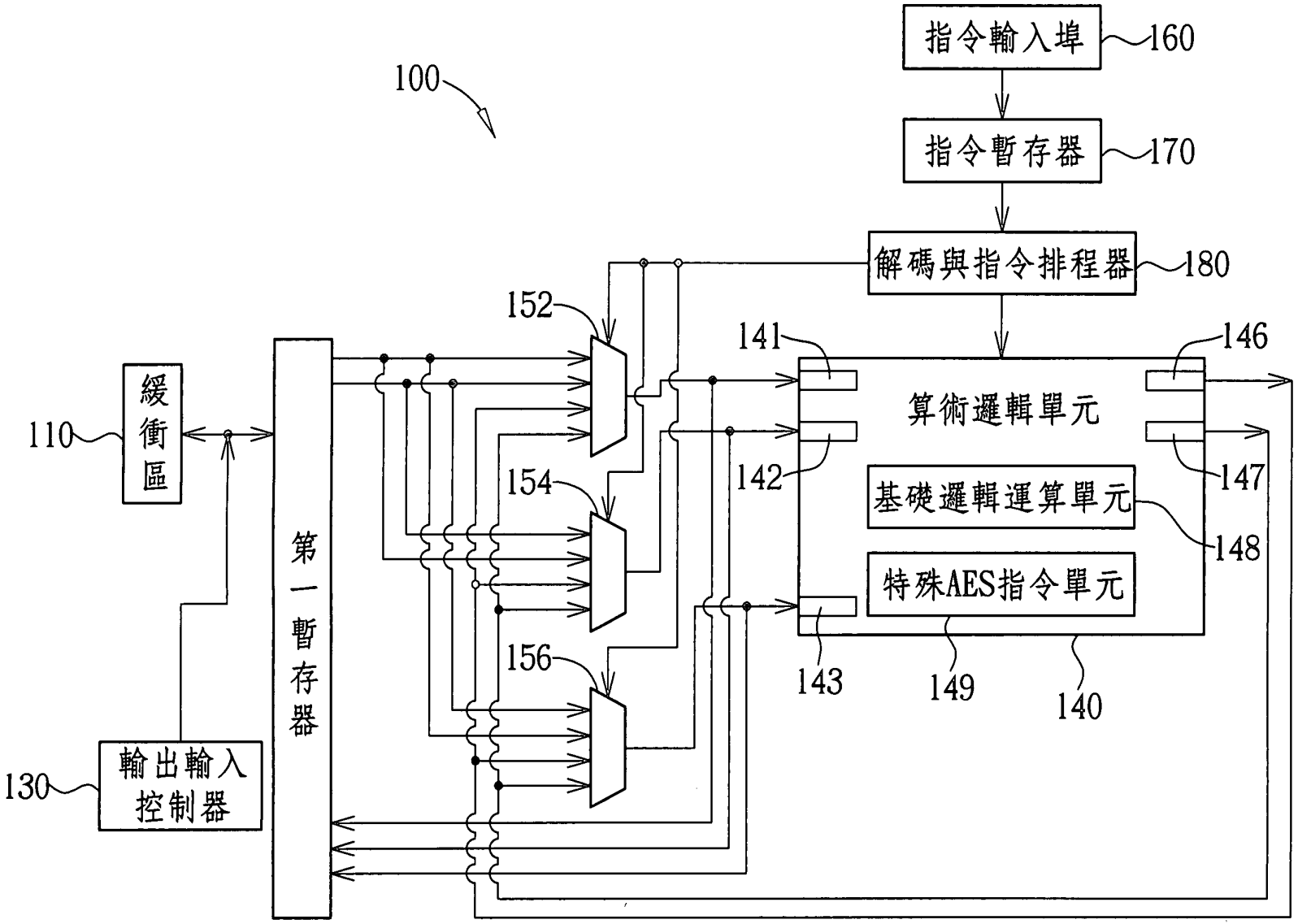
19. 如申請專利範圍第18項之方法，其可執行一逆替換位元組換列-4(inverse substitute byte shift row 4, INVSBSR4) 指令，且該方法於執行該逆替換位元組換列-4指令時係同時處理暫存於該暫存器R20、該暫存器



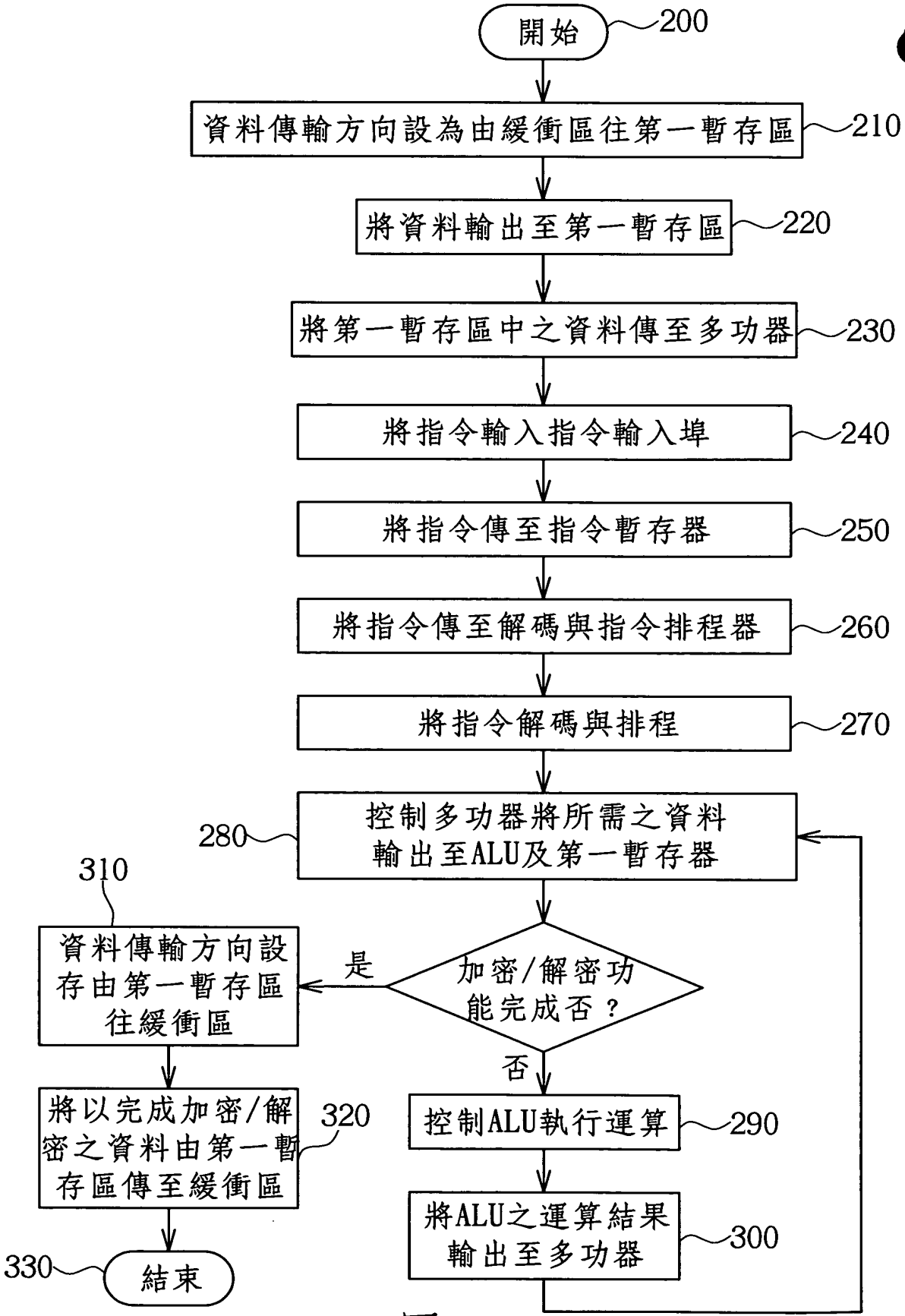
R21、該暫存器R22及該暫存器R3之最高有效位元組（most significant byte, MSB）及第二高有效位元組共八個位元組之資料。

20. 如申請專利範圍第1項之方法，其可執行包含偏碼表（Offset Code Book, OCB)模式以及Counter mode with CBC MAC (CCM)模式之進階密碼標準之加解密功能。

21. 如申請專利範圍第1項之方法，其可使用同樣的密鑰同時對複數筆資料進行加密。


100
指令輸入埠
160
指令暫存器
170
解碼與指令排程器
180
152
154
156
141
146
算術邏輯單元
142
147
基礎邏輯運算單元
148
特殊AES指令單元
143
149
140
110
緩衝區
第一暫存器
130
輸出輸入控制器

圖一


開始
200
資料傳輸方向設為由緩衝區往第一暫存區
210
將資料輸出至第一暫存區
220
將第一暫存區中之資料傳至多功器
230
將指令輸入指令輸入埠
240
將指令傳至指令暫存器
250
將指令傳至解碼與指令排程器
260
將指令解碼與排程
270
280
控制多功器將所需之資料輸出至ALU及第一暫存器
加密/解密功能完成否？
是
否
310
資料傳輸方向設存由第一暫存區往緩衝區
將以完成加密/解密之資料由第一暫存區傳至緩衝區
320
控制ALU執行運算
290
將ALU之運算結果輸出至多功器
300
330
結束

圖二

第 1/27 頁

第 1/27 頁

第 2/27 頁

第 3/27 頁

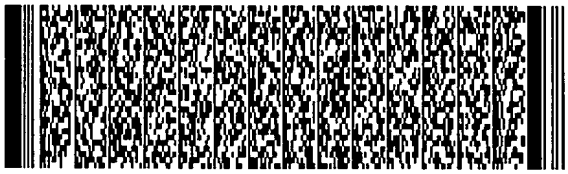
第 3/27 頁

第 4/27 頁

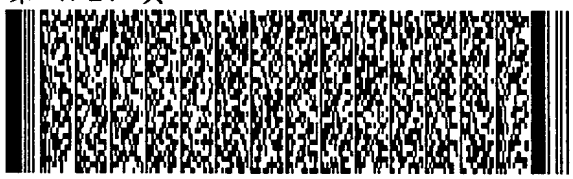
第 5/27 頁

第 6/27 頁

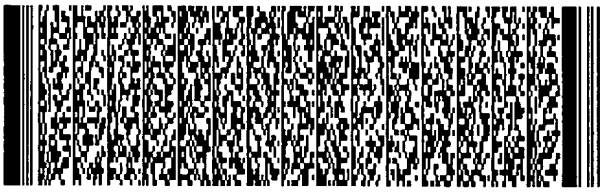
第 7/27 頁



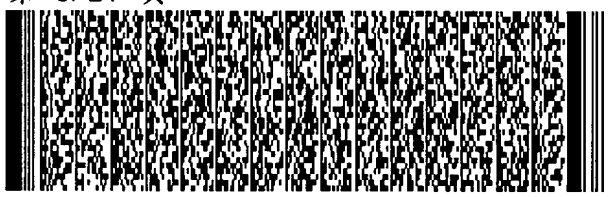
第 7/27 頁



第 8/27 頁



第 8/27 頁



第 9/27 頁

第 9/27 頁

第 10/27 頁

第 10/27 頁

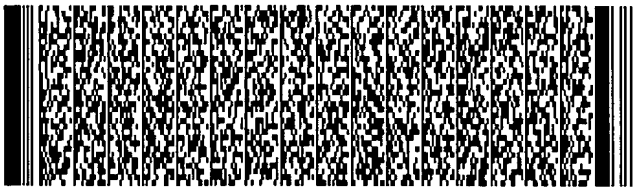
第 11/27 頁

第 11/27 頁

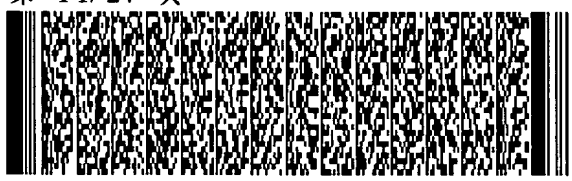
第 12/27 頁

第 12/27 頁

第 13/27 頁



第 14/27 頁

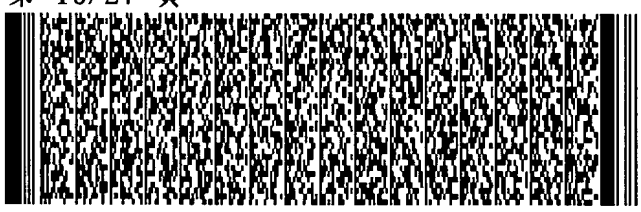


第 14/27 頁

第 15/27 頁

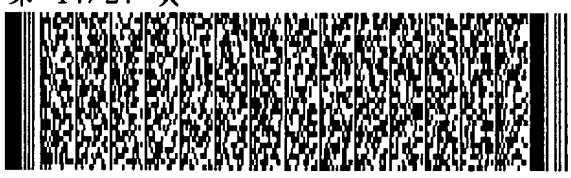
第 15/27 頁

第 16/27 頁



第 17/27 頁

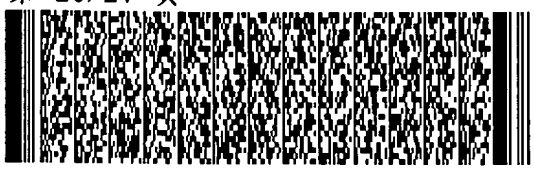
第 17/27 頁



第 18/27 頁

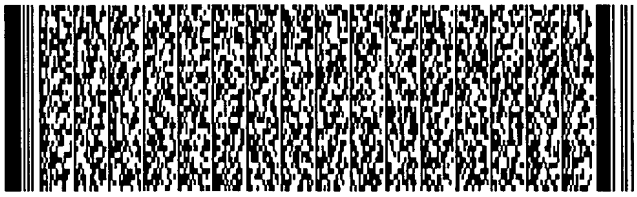
第 19/27 頁

第 20/27 頁

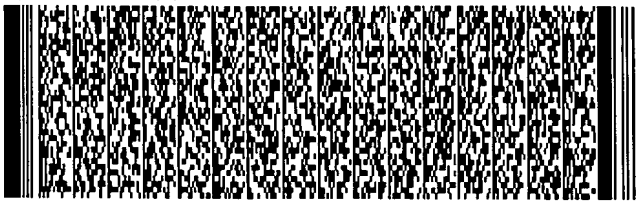


第 20/27 頁

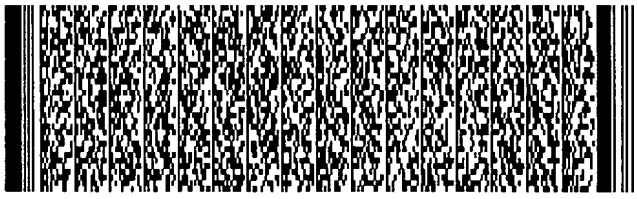
第 21/27 頁



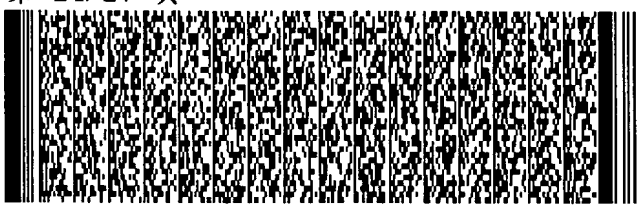
第 22/27 頁



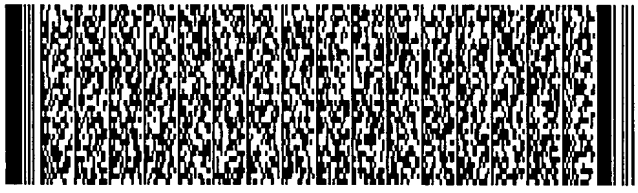
第 23/27 頁



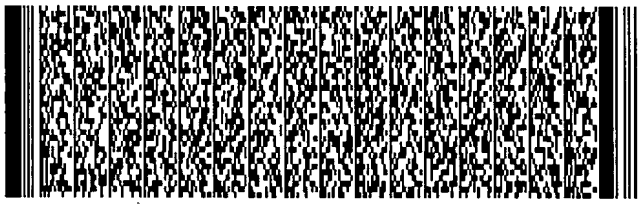
第 24/27 頁



第 25/27 頁



第 26/27 頁



第 27/27 頁